CLAIM AMENDMENTS

1. (CURRENTLY AMENDED) A multi-function peripheral device comprising:

a network interface configured to allow the multi-function peripheral device to communicate with network devices over a network;

a graphical user interface configured to allow for the exchange of information between the multi-function peripheral device and a user;

one or more processors;

a memory;

a scan process executing in the memory and being configured to cause a printed document to be scanned at the multi-function peripheral device and to generate scan data that includes a digital data representation of ~~the~~ a first electronic document that is based on the printed document;

a print process executing in the memory and being configured to process print data and cause a printed version of ~~an~~ a second electronic document reflected in the print data to be generated by the multi-function peripheral device at the multi-function peripheral device; and

a virus protection process executing in the memory and being configured to perform the steps of:

examine data stored on non-volatile memory of the multi-function peripheral device;

based on examining the data, detect that one or more unauthorized instructions ~~have been~~ are stored on the non-volatile memory of the multi-function peripheral device; and

in response to detecting that the one or more unauthorized instructions have been stored on the non-volatile memory of the multi-function peripheral device[[,]]:

perform one or more actions to address the one or more unauthorized instructions that have been stored on the non-volatile memory of the multi-function peripheral device; and

wherein the one or more actions includes rendering the one or more unauthorized instructions inaccessible and unexecutable on the multi-function peripheral device by moving the one or more unauthorized instructions into a protected area of the non-volatile memory.

2. (PREVIOUSLY PRESENTED) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is configured to detect that the one or more unauthorized instructions have been stored on the multi-function peripheral device by periodically examining, according to specified configuration criteria, data stored on the multi-function peripheral device to determine whether the data has been modified in an unauthorized manner.

3. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is configured to detect that the one or more unauthorized instructions have been stored on the multi-function peripheral device by examining and detecting the modification of data ~~that one or more data files~~ stored on the multi-function peripheral device, wherein the data is selected from the group consisting of one or more data files, program code, and configuration data. ~~have been modified.~~

4. (CANCELLED)

5. (CANCELLED)

6. (CANCELLED)

7. (CANCELLED)

8. (ORIGINAL) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is further configured to undo changes made as a result of execution of the one or more unauthorized instructions.

9. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is further configured to:

determine whether particular data stored on the multi-function peripheral device can be restored to a prior state; and

in response to determining that the particular data cannot be restored to the prior state, then delete the particular data from the multi-function peripheral device.

10. (CANCELLED)

11. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is further configured to ~~notify~~ provide a notification ~~a user via the graphical user interface on the multi-function peripheral device~~ that the storage

of the one or more unauthorized instructions on the multi-function peripheral device has been detected, wherein the notification is selected from the group consisting of displaying information on the graphical user interface on the multi-function peripheral device, printing a report on the multi-function peripheral device, sending an email from the multi-function peripheral device, and sending a facsimile from the multi-function peripheral device.

12. (CANCELLED)

13. (CANCELLED)

14. (CANCELLED)

15. (PREVIOUSLY PRESENTED) The multi-function peripheral device as recited in Claim 1, wherein the multi-function peripheral device is configured to receive, over a network, data used by the virus protection process to detect that the one or more unauthorized instructions have been stored on the multi-function peripheral.

16. (NEW) The multi-function peripheral device as recited in Claim 1, wherein:
the one or more unauthorized instructions are contained in a file stored on a portion of the non-volatile memory;
the one or more actions includes deleting the file; and
the virus protection process is further configured to, after deleting the file, overwrite the portion of the non-volatile memory with a specified pattern.

17. (NEW) A multi-function peripheral device comprising:
a network interface configured to allow the multi-function peripheral device to communicate with network devices over a network;
a graphical user interface configured to allow for the exchange of information between the multi-function peripheral device and a user;
one or more processors;
a memory;
a scan process executing in the memory and being configured to cause a printed document to be scanned at the multi-function peripheral device and to generate scan data that includes a digital data representation of a first electronic document that is based on the printed document;

a print process executing in the memory and being configured to process print data and cause a printed version of a second electronic document reflected in the print data to be generated by the multi-function peripheral device at the multi-function peripheral device; and

a virus protection process executing in the memory and being configured to, upon receipt of data by the multi-function peripheral device from a network device over the network, perform the steps of:

examine the data to determine whether the data contains one or more unauthorized instructions;

in response to determining that the data contains one or more unauthorized instructions, perform one or more actions on the data to protect the multi-function peripheral device; and

wherein the one or more actions includes rendering the one or more unauthorized instructions inaccessible and unexecutable on the multi-function peripheral device by moving the unauthorized instructions into a protected area of non-volatile memory.

18. (NEW) The multi-function peripheral device recited in Claim 17, wherein:

the virus protection process is further configured to generate and provide a notification that the multi-function peripheral device received the data containing the one or more unauthorized instructions;

the notification is selected from the group consisting of displaying information on the graphical user interface on the multi-function peripheral device, printing a report on the multi-function peripheral device, sending an email, and sending a facsimile; and

the one or more unauthorized instructions are unauthorized executable program code.

19. (NEW) The multi-function peripheral device as recited in Claim 17, wherein:

the one or more unauthorized instructions are contained in a file stored on a portion of the non-volatile memory;

the one or more actions includes deleting the file; and

the virus protection process is further configured to, after deleting the file, overwrite the portion of the non-volatile memory with a specified pattern.

20. (NEW) A multi-function peripheral device comprising:

a network interface configured to allow the multi-function peripheral device to communicate with network devices over a network;

a graphical user interface configured to allow for the exchange of information between the multi-function peripheral device and a user;

one or more processors;

a memory;

a scan process executing in the memory and being configured to cause a printed document to be scanned at the multi-function peripheral device and to generate scan data that includes a digital data representation of a first electronic document that is based on the printed document;

a print process executing in the memory and being configured to process print data and cause a printed version of a second electronic document reflected in the print data to be generated by the multi-function peripheral device at the multi-function peripheral device; and

a virus protection process executing in the memory and being configured to, prior to sending data from the multi-function peripheral device to a network device over the network, perform the steps of:

examine the data to determine whether the data contains one or more unauthorized instructions;

in response to determining that the data contains one or more unauthorized instructions, perform one or more actions; and

wherein the one or more actions includes rendering the one or more unauthorized instructions inaccessible and unexecutable on the multi-function peripheral device by moving the unauthorized instructions into a protected area of non-volatile memory.

21. (NEW) The multi-function peripheral device recited in Claim 20, wherein the one or more actions include not sending the data to the network device.

22. (NEW) The multi-function peripheral device recited in Claim 20, wherein:

the one or more actions include generating and providing a notification that indicates that the multi-function peripheral device has the data that has been infected by a virus;

the notification is selected from the group consisting of displaying information on the graphical user interface on the multi-function peripheral device, printing a report on the multi-function peripheral device, sending an email, and sending a facsimile;

the one or more unauthorized instructions are unauthorized executable program code; and

the virus protection process is configured to detect that one or more unauthorized instructions have been stored on the multi-function peripheral device by examining and detecting that the data has been modified.

23. (NEW) The multi-function peripheral device as recited in Claim 20, wherein the data is stored on a portion of the memory of the multi-function peripheral device, wherein the portion of the memory is selected from the group consisting of a portion of non-volatile memory and a portion of volatile memory.

24. (NEW) The multi-function peripheral device as recited in Claim 20, wherein the virus protection process is further configured to undo changes made as a result of execution of the one or more unauthorized instructions.

25. (NEW) The multi-function peripheral device as recited in Claim 20, wherein the virus protection process is further configured to:

determine whether the data stored on the multi-function peripheral device can be restored to a prior state; and

in response to determining that the data cannot be restored to the prior state, delete the data from the multi-function peripheral device.

26. (NEW) The multi-function peripheral device as recited in Claim 20, wherein:

the one or more unauthorized instructions are contained in a file stored on a portion of the non-volatile memory;

the one or more actions includes deleting the file; and

the virus protection process is further configured to, after deleting the file, overwrite the portion of the non-volatile memory with a specified pattern.

27. (NEW) The multi-function peripheral device as recited in Claim 20, wherein the virus protection process is further configured to provide a notification on the multi-function peripheral device that the data contains one or more unauthorized instructions, wherein the

notification is selected from the group consisting of displaying information on the graphical user interface on the multi-function peripheral device, printing a report on the multi-function peripheral device, sending an email from the multi-function peripheral device, and sending a facsimile from the multi-function peripheral device.

28. (NEW) The multi-function peripheral device as recited in Claim 20, wherein the multi-function peripheral device is configured to receive, over a network, data used by the virus protection process to detect that the one or more unauthorized instructions have been stored on the multi-function peripheral device.